HIPAA SECURITY RISK ANALYSIS FOR UINTAH BASIN HEALTHCARE 2022

Date: Feb 17, 2023

For:
Uintah Basin Healthcare 2022
250 West 300 North
Roosevelt, UT 84066
Cerner

Table of Contents

EXHIBIT
13

Letter of HIPAA Security Risk Analysis Completion

Feb 17, 2023

Uintah Basin Healthcare 2022
250 West 300 North
Roosevelt, UT 84066

Dear Preston Marx,

Based upon representation from management as to the accuracy and completeness of information provided during the HIPAA Risk Analysis and the procedures performed by Intraprise Health, the following organization has been audited:

Uintah Basin Healthcare 2022

The completed HIPAA Risk Analysis was sent to Uintah Basin Healthcare 2022 Management for circulation, review and final validation.

Intraprise Health assessments allow both healthcare organizations and their business associates to realize the benefits of more assurance by aligning with best practices and leveraging the NIST 800-30 Risk Management Guide, COBIT, HITECH and HIPAA regulations. Intraprise Health assessments are designed to occur along an incremental path towards compliance and an ongoing Risk Management process. Organizations can actively move along the HIPAA and HITECH compliance path in a measured way, while realizing at an early stage the benefits of a common means to assess security controls and communicate compliance.

Please do not hesitate to contact your assigned security consultant or call us at 801.770.1199, should you have any questions or comments.

Thank you for this opportunity to assist Uintah Basin Healthcare 2022 in pursuing HIPAA and HITECH compliance and the overall Risk Management effort.

Sincerely,

Intraprise HEALTH + HIPAA One

Introduction

In order to better protect Uintah Basin Healthcare 2022's sensitive information, and to comply with the Health Insurance Portability and Accountability Act (HIPAA), Intraprise Health conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the electronic protected health information it holds. This assessment was initially performed on Nov 4, 2022 through Feb 17, 2023, and will be updated annually by the organization.

Scope 1

The scope of this assessment encompasses 1 HIPAA Security Risk Analysis covering Technical, Administrative, Organizational and Physical safeguards for:

1 Organization: Uintah Basin Healthcare 2022: 250 West 300 North, Roosevelt, UT 84066

1 Primary ePHI system: Cerner managed by Marcy McDonald and Kashell Verholtz

4 additional ePHI systems:

- Clarity managed by Preston Marx,
- Harmony - Health Data Archive managed by Kashell Verholtz,
- T-System managed by Marcy McDonald, and
- Point Click Care managed by Kashell Verholtz.

1 additional remote location:

- Uintah Basin Healthcare - Vernal Campus, 379 N 500 W, Vernal, UT 84078.

Each location and ePHI System adds questions requiring supporting documentation to prove compliance, and full risk analysis for any gaps in compliance discussed in the following sections.

Definitions

Electronic Personal Health Information (ePHI or PHI): Individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium. This information must relate to any of the following:

The past, present or future physical or mental health or condition of an individual

Provision of healthcare to an individual

Payment for the provision of healthcare to an individual

If the information identifies or provides a reasonable basis to believe it can be used to identify an individual, it is considered individually identifiable health information. Elements that make health information individually identifiable include, but are not limited to, the following:

Name

Telephone/fax number

E-mail address

Social Security number

Driver’s license number

Internet Address

Any other unique identifying number characteristic or code

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally or intentionally) and result in a security breach to PHI.

Threat: The potential for an event and/or individual to exercise a specific vulnerability.

Risk: The impact on Uintah Basin Healthcare 2022, considering (1) the probability that a particular threat will exercise a particular vulnerability and (2) the resulting impact if this should occur. Risk = Threat X Vulnerability X Cost

Control: A measure—technical or manual—of reducing the risk to Uintah Basin Healthcare 2022.

Risk Assessment Approach

The risk assessment was performed with Preston Marx, Danelle Brinkerhoff, David Benson, Craig Zobell, Kenny Stansfield, Kashell Verholtz and Marcy McDonald. The participants used their knowledge of Uintah Basin Healthcare 2022's operations, their expertise in the IT, security and healthcare fields to complete the risk assessment. Vulnerability information was taken from the National Vulnerability Database at the National Institute for Standards and Technology (NIST) and from scans generated from the Nessus Professional-Feed Vulnerability Scans. An inventory was gathered from scans performed during the assessment.

Methodology

The Office for Civil Rights (OCR) suggested assessment methodology that provides a subjective analysis and conclusions based on the control objectives for the National Institute of Standards and Technology was used; namely the NIST 800-30 publication. For an organization of Uintah Basin Healthcare 2022's size, this framework is the suggested framework from the HIPAA Security Rule and was the methodology used to ensure compliance and due-diligence for Uintah Basin Healthcare 2022.

We also employed the HITECH Act, HIPAA and COBIT framework mixed with best practices and current exploit reports from syndicated exploit news groups.

HIPAA Security Compliance Discussion

The risk assessment included consideration of all “required” safeguards identified within HIPAA. Based upon representation from management as to the accuracy and completeness of the information provided in the HIPAA One® Questionnaire, the following safeguards were deemed to be compliant:

Scope Clause / Citation	Safeguard Included Comments and Attachments
Uintah Basin Healthcare Clarity 164.308(a)(1)(i), AC-4 CA-3 CA-9 PL-8 SA-9(2) Security Management Process	**Section:** administrative **Specification:** Security Management Process **HIPAA One® Question:** Do you have a list or diagram detailing ALL the EMR/ePHI /PII Database interfaces including type of interface (e.g. HL-7, other persistent DB connections, etc.) including their destination, direction, internal/external, and purpose? **Included Comments:** The only interface is with the B-Braun dialysis machines in the clinic and personal identifying information is not shared with the machines. Continues same, 10/4/2021 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** Interfaces connections.docx
Uintah Basin Healthcare Point Click Care 164.308(a)(1)(i), AC-4 CA-3 CA-9 PL-8 SA-9(2) Security Management Process	**Section:** administrative **Specification:** Security Management Process **HIPAA One® Question:** Do you have a list or diagram detailing ALL the EMR/ePHI /PII Database interfaces including type of interface (e.g. HL-7, other persistent DB connections, etc.) including their destination, direction, internal/external, and purpose? **Included Comments:** Therapute is the only interface. HIPAA One Analysis: Verified PM 10/29/19 --Updates below this line were imported from the Action History Page. Edit as needed-- --This question has been remediated in the previous assessment. Please see below for details.-- 02-05-2020 - Interfaces Documented Jennifer Aumiller KV 09/28/21 PM 2022 **Attachments:** Interfaces with PointClickCare.docx
Uintah Basin Healthcare T-System 164.308(a)(1)(i), AC-4 CA-3 CA-9 PL-8 SA-9(2) Security Management Process	**Section:** administrative **Specification:** Security Management Process **HIPAA One® Question:** Do you have a list or diagram detailing ALL the EMR/ePHI /PII Database interfaces including type of interface (e.g. HL-7, other persistent DB connections, etc.) including their destination, direction, internal/external, and purpose? **Included Comments:** HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** T-System interfaces.PNG

Organization 164.308(a)(1)(i), AU-1 CA-2 CA-7 RA-1(c) Security Management Process	**Section:** administrative **Specification:** Security Management Process **HIPAA One® Question:** Security Violations - has the Organization defined the frequency of its Risk Assessment review and updates? **Included Comments:** Annual risk assessment. findings are shared with senior leadership and board of trustees. PM 10/21 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** ITS Security Policy 1.3.pdf
Organization 164.308(a)(1)(i), AU-1 through AU-6 CA-1 CA-2 RA-1 PM-1 PM-2 Security Management Process	**Section:** administrative **Specification:** Security Management Process **HIPAA One® Question:** Security Violations - does the Organization have Policies and Procedures (PnP) for the assigning of roles, prevention, detection, countermeasures, containment and correction of security violations? **Included Comments:** Policies reviewed. valid until 2023. PM HIPAA One Analysis: 11.3.2021 PM PM 2022 **Attachments:** ITS Employee Account Policy 4.2.pdf ITS Security Policy 1.3.pdf
Uintah Basin Healthcare Cerner 164.308(a)(1)(i), CM-8 PM-29 Security Management Process	**Section:** administrative **Specification:** Security Management Process **HIPAA One® Question:** Can you provide an accurate count on how many individual patient records exist in this EMR/ePHI/PII system? **Included Comments:** The total number of FINs is 2,032,066 and the total number of MRNs is 30,9984 KV 10/05/21 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** MRNS&FINS.PNG
Uintah Basin Healthcare T-System 164.308(a)(1)(i), CM-8 PM-29 Security Management Process	**Section:** administrative **Specification:** Security Management Process **HIPAA One® Question:** Can you provide an accurate count on how many individual patient records exist in this EMR/ePHI/PII system? **Included Comments:** 172,576 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:**
Uintah Basin Healthcare Clarity 164.308(a)(1)(i), CM-8 PM-29 Security Management Process	**Section:** administrative **Specification:** Security Management Process **HIPAA One® Question:** Can you provide an accurate count on how many individual patient records exist in this EMR/ePHI/PII system? **Included Comments:** Individual patient records - 642 10/4/2021 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:**

Uintah Basin Healthcare Point Click Care 164.308(a)(1)(i), CM-8 PM-29 Security Management Process	**Section:** administrative **Specification:** Security Management Process **HIPAA One® Question:** Can you provide an accurate count on how many individual patient records exist in this EMR/ePHI/PII system? **Included Comments:** The total number of FINs is 1,597,590 and the total number of MRNs is 271,465. KV 10/05/21 HIPAA One Analysis: PM 2022 **Attachments:**
Uintah Basin Healthcare 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(d), AC-19 CA-8-9 CM-12 MP-1 MP-4 MP-7 PM-5 PM-29 SA-1 SA-4 Security Management Process	**Section:** administrative **Specification:** Security Management Process **HIPAA One® Question:** For this location - Does the organization have a Policy and Procedure (PnP) and an inventory of ALL systems housing ePHI? Specifically, the servers, laptops, desktops, tablets, smartphones and removable media (e.g. USB drives, DVD, etc.) that contain or access ePHI? Server, PC and mobile device Inventory must include at a minimum: hostname, O/S version with Service Pack and brief description for each (3 columns). **Included Comments:** No Change. 11-8-2021 C Zobell The bulk of our ePHI is managed by Cerner for us. We do have some legacy EHR's that we should have inventoried. Update 11-7-2018: We no longer have any locally stored ePHI. There is nothing to inventory. CZ HIPAA One Analysis:11.5.2021 PM PM 2022 **Attachments:** Endpoint Security Procedure.pdf ITS Acceptable Use Policy 3.1.pdf
Uintah Basin Healthcare - Vernal Campus 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(d), AC-19 CA-8-9 CM-12 MP-1 MP-4 MP-7 PM-5 PM-29 SA-1 SA-4 Security Management Process	**Section:** administrative **Specification:** Security Management Process **HIPAA One® Question:** For this location - Does the organization have a Policy and Procedure (PnP) and an inventory of ALL systems housing ePHI? Specifically, the servers, laptops, desktops, tablets, smartphones and removable media (e.g. USB drives, DVD, etc.) that contain or access ePHI? Server, PC and mobile device Inventory must include at a minimum: hostname, O/S version with Service Pack and brief description for each (3 columns). **Included Comments:** No Change. 11-8-2021 C Zobell ePHI isn't stored locally. It is all remote hosted. Same as previous question. We have no local ePHI systems. There is nothing to inventory. CZ HIPAA One Analysis:11.5.2021 PM PM 2022 **Attachments:** Endpoint Security Procedure.pdf ITS Acceptable Use Policy 3.1.pdf

Organization 164.308(a)(1)(ii)(A), AU-1 CA-1 CA-2 RA-1 RA-2 RA-3 RA-7 Security Management Process	**Section:** administrative **Specification:** Risk Analysis **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place and has previously conducted a HIPAA Risk Analysis or any other type of Risk Analysis? **Included Comments:** Added 2020 Risk Assessment. PM 10/21 HIPAA One Analysis:11.3.2021 PM Added 2021 Risk Assessment. PM 2022 **Attachments:** 2014 UBH Risk Assessment.pdf 2015 UBH HIPAAOneAssessment.pdf 2016 UBH HIPAAOneAssessment.pdf 2017 UBH HIPAAOneAssessment.pdf 2018 UBH HIPAAOneAssessment.pdf 2019 UBH HIPAAOneAssessment.pdf 2020 UBH HIPAAOneAssessment.pdf 2021 UBH HIPAAOneAssessment.pdf ITS Security Policy 1.3.pdf UBH HIPPA Security Response 2014.pdf
Organization 164.308(a)(1)(ii)(A), RA-5 Security Management Process	**Section:** administrative **Specification:** Risk Analysis **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) requiring an annual external server and network vulnerability scan on Internet-facing devices? **Included Comments:** Verbiage requiring an annual external vulnerability scan was added to the network management policy. UBH Verified PM HIPAA One Analysis: 11.3.2021 **Attachments:** Network Management Policy 2.2.pdf
Organization 164.308(a)(1)(ii)(B), CA-1 CA-5 CA-7 PM-9 PM-31 PM-32 RA-3 RA-7 Security Management Process	**Section:** administrative **Specification:** Risk Management **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place for documented security updates OR updates on progress from previous HIPAA or any other Risk Analysis recommendations? **Included Comments:** Added 2020 Risk Assessment. PM 10/21 HIPAA One Analysis:11.3.2021 PM Added 2021 Risk Assessment. PM 2022 **Attachments:** 2013 UBH HIPPA Security Response.pdf 2015 UBH HIPAAOneAssessment.pdf 2016 UBH HIPAAOneAssessment.pdf 2017 UBH HIPAAOneAssessment.pdf 2018 UBH HIPAAOneAssessment.pdf 2019 UBH HIPAAOneAssessment.pdf 2020 UBH HIPAAOneAssessment.pdf 2021 UBH HIPAAOneAssessment.pdf ITS Security Policy 1.3.pdf UBH HIPPA Security Response 2014.pdf

Organization 164.308(a)(1)(ii)(C), PM-12 PS-8 (a) Security Management Process	**Section:** administrative **Specification:** Sanction Policy **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) for applying worker sanctions (i.e. termination, leave of absence, pay raise holdings for non-completion of HIPAA training, etc.) for violating any security or HIPAA-related Policies and Procedures? **Included Comments:** Attached Sanctioning Workforce PDF file shows tiered levels of sanctions for violating HIPAA policies. HIPAA One Analysis:11.3.2021 **Attachments:** Copy of Sanctioning Workforce members who Violate Privacy Policies.pdf
Organization 164.308(a)(1)(ii)(D), 164.312(a)(2)(i), 164.312(b), AC-1 AC-2 AU-2-14 IA-1 IA-2 SI-1 Security Management Process	**Section:** administrative **Specification:** Information System Activity Review. **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place to assign unique user IDs (including not sharing accounts, ensuring all user IDs are associated with a person) and periodically review EMR/ePHI/PII record access logs (i.e. to show who accessed a patient's chart and who is logged into the system) at a set interval? **Included Comments:** We have a monthly HIPAA Advisory committee meeting comprised of: HIPAA Privacy Officer - Angie Draper HIPAA Security Officer - Preston Marx VP of Quality - Roger Burton We will run audits prior to that meeting of the Cerner system. We typically run the audit based on probable cause so the randomness of our audits could be improved. Updated Security and Account policy to stated that our audit will ensure unique accounts are used. 10/21 PM HIPAA One Analysis:11.3.2021 PM **Attachments:** EMR chart audit.PNG ITS Employee Account Policy 4.2.pdf ITS Security Policy 1.3.pdf
Organization 164.308(a)(2), AC-1(b) RA-1(b) CA-1(b) Assigned Security Responsibility	**Section:** administrative **Specification:** Assigned Security Responsibility **HIPAA One® Question:** Does the organization have an assigned person to be the HIPAA Security Officer and is responsible for maintaining HIPAA Security Policies and Procedures (PnP)? **Included Comments:** Preston Marx VP Information Technology HIPAA One Analysis:11.3.2021 **Attachments:** VP IT.pdf

Organization 164.308(a)(2), PM-2 Assigned Security Responsibility	**Section:** administrative **Specification:** Assigned Security Responsibility **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) along with a job description for the HIPAA Security Officer that includes the responsibility to maintain HIPAA Security Policies and Procedures? **Included Comments:** Added paragraph to security policy that describes the role of the security officer. PM 11/15/2021. **Attachments:** ITS Security Policy 1.2.pdf ITS Security Policy 1.4.pdf Revenue Integrity Manager .pdf VP IT.pdf
Organization 164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.312(d), AC-1(a)(1) AC-4 PS-3 Workforce Security	**Section:** administrative **Specification:** Workforce Security **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place to authorize and grant new user access OR change existing user access to the EMR/ePHI/PII and/or RIS/PACS systems (i.e. to verify that a person seeking access to ePHI is the one claimed)? **Included Comments:** Employee account policy updated and uploaded. It reiterates that managers authorize access, ITS grants it. PM 10/21 HIPAA One Analysis: 11.3.2021 PM PM 2022 **Attachments:** ITS Employee Account Policy 4.2.pdf
Uintah Basin Healthcare Point Click Care 164.308(a)(3)(ii)(A), AC-2(e) AC-24 PS-3 Workforce Security	**Section:** administrative **Specification:** Authorization and/or Supervision **HIPAA One® Question:** Are users who have access to any EMR/ePHI/PII systems authorized and approved by their department head or supervisor before granted access? **Included Comments:** Access is granted per supervisor approval when an email is received by Amanda Hartman, Administrator at the Villa. She may delegate that access to another to actually create the accounts within Point Click Care. Verified KV 09/28/21 PM 2022 User list was provided by Villa Administrator, discussed with the VP ITS and determined to be accurate. HIPAA One Analysis:11.3.2021 PM **Attachments:** ITS Employee Account Policy 4.1.pdf
Uintah Basin Healthcare Clarity 164.308(a)(3)(ii)(A), AC-2(e) AC-24 PS-3 Workforce Security	**Section:** administrative **Specification:** Authorization and/or Supervision **HIPAA One® Question:** Are users who have access to any EMR/ePHI/PII systems authorized and approved by their department head or supervisor before granted access? **Included Comments:** Continues the same. The manager enters and disables any employees as they are hired and terminated. 11/01/2020 Continues same, 10/4/2021 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** new+employee+form.pdf

Uintah Basin Healthcare Cerner 164.308(a)(3)(ii)(A), AC-2(e) AC-24 PS-3 Workforce Security	**Section:** administrative **Specification:** Authorization and/or Supervision **HIPAA One® Question:** Are users who have access to any EMR/ePHI/PII systems authorized and approved by their department head or supervisor before granted access? **Included Comments:** The department manager completes the new employee ticket and writes in what current employee to model the new employee's access after. We have to have this ticket before the account can be created. KV 10/05/21 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** new employee ticket.PNG
Uintah Basin Healthcare T-System 164.308(a)(3)(ii)(A), AC-2(e) AC-24 PS-3 Workforce Security	**Section:** administrative **Specification:** Authorization and/or Supervision **HIPAA One® Question:** Are users who have access to any EMR/ePHI/PII systems authorized and approved by their department head or supervisor before granted access? **Included Comments:** When a new employee is hired, the ED Manager fills out the IT new employee form and lists which current employee the new employee should be built after and what access the new employee needs. HIPAA One Analysis: 11.3.2021 PM PM 2022 **Attachments:** ITS Employee Account Policy 4.2.pdf new employee ticket.PNG
Uintah Basin Healthcare Harmony - Health Data Archive 164.308(a)(3)(ii)(A), AC-2(e) AC-24 PS-3 Workforce Security	**Section:** administrative **Specification:** Authorization and/or Supervision **HIPAA One® Question:** Are users who have access to any EMR/ePHI/PII systems authorized and approved by their department head or supervisor before granted access? **Included Comments:** Users that have/need access to the EMR/ePHI/PII managers /supervisor will put in an IT request asking to get them access. Which then goes to our IT ticketing system. KV 09/28/21 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** 90- new employee form.pdf ITS Employee Account Policy 4.2.pdf NewHireTicket.PNG
Uintah Basin Healthcare Point Click Care 164.308(a)(3)(ii)(B), AC-3(7) AC-6 Workforce Security	**Section:** administrative **Specification:** Workforce Clearance Procedure **HIPAA One® Question:** Is access to EMR/ePHI/PII records granted on the principle of minimal access (or "need to know") needed to perform their job function? **Included Comments:** Each employee is put into the "Module" that fits their job function. Verified KV 09/28/21 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** ITS Employee Account Policy 4.2.pdf SecurityGroupPCC.JPG

Uintah Basin Healthcare Clarity 164.308(a)(3)(ii)(B), AC-3(7) AC-6 Workforce Security	**Section:** administrative **Specification:** Workforce Clearance Procedure **HIPAA One® Question:** Is access to EMR/ePHI/PII records granted on the principle of minimal access (or "need to know") needed to perform their job function? **Included Comments:** Continues same, 10/4/2021 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** Minimal access.docx
Uintah Basin Healthcare Cerner 164.308(a)(3)(ii)(B), AC-3(7) AC-6 Workforce Security	**Section:** administrative **Specification:** Workforce Clearance Procedure **HIPAA One® Question:** Is access to EMR/ePHI/PII records granted on the principle of minimal access (or "need to know") needed to perform their job function? **Included Comments:** Yes, users start with basic access and then we grant more access as needed for their job function. KV 10/05/21 HIPAA One Analysis: 11.3.2021 PM PM 2022 **Attachments:** CAH medical records (1).PNG CAH RN (1).PNG ITS Employee Account Policy 4.2.pdf
Uintah Basin Healthcare T-System 164.308(a)(3)(ii)(B), AC-3(7) AC-6 Workforce Security	**Section:** administrative **Specification:** Workforce Clearance Procedure **HIPAA One® Question:** Is access to EMR/ePHI/PII records granted on the principle of minimal access (or "need to know") needed to perform their job function? **Included Comments:** The ED manager lists a current employee that works in the same position that the new employee has been hired from; the new employee is granted the same access as the current employee. HIPAA One Analysis:11.3.2021 PM **Attachments:** t system position guide.docx Tsystem Privileges.PNG Tsystem2022Audit.PNG
Uintah Basin Healthcare Harmony - Health Data Archive 164.308(a)(3)(ii)(B), AC-3(7) AC-6 Workforce Security	**Section:** administrative **Specification:** Workforce Clearance Procedure **HIPAA One® Question:** Is access to EMR/ePHI/PII records granted on the principle of minimal access (or "need to know") needed to perform their job function? **Included Comments:** Access is granted through AD security group membership. These SG's grant access by data source within Health Data Archive. We do audits of the system and remove all user accounts that have not been accessed in the system. KV 09/28/21 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** CPSI roles.PNG harmony_access_groups.PNG

Organization 164.308(a)(3)(ii)(B), PS-2 PS-3 Workforce Security	**Section:** administrative **Specification:** Workforce Clearance Procedure **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) to ensure that during the hiring process, some type of employment background check is performed on potential job candidates? **Included Comments:** Applicants are notified in the application process that they will need to complete a successful background check and must acknowledge before they can proceed. Once a job offer is made the candidate is contacted to complete a background authorization. If the candidates background authorization is successful we continue with the on-boarding process. The background check is included on the New Employee Information Sheet as being completed and everything is kept in the employment file. HIPAA One Analysis:11.3.2021 **Attachments:** Blue line Release Form.pdf NEWHIRE EMPLOYEE INFORMATION SHEET.pdf Pre Application Consent.pdf Recruitment & Hiring Practices Policy.pdf
Organization 164.308(a)(3)(ii)(B), PS-6 Workforce Security	**Section:** administrative **Specification:** Workforce Clearance Procedure **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) that requires new hires to sign a confidentiality agreement? **Included Comments:** HIPAA One Analysis:11.3.2021 **Attachments:** Confidentiality Policy.pdf Workforce Privacy Agreement.docx
Uintah Basin Healthcare T-System 164.308(a)(3)(ii)(C), 164.310(a)(2)(iii), AC-2(g)(12) Workforce Security	**Section:** administrative **Specification:** Termination Procedures **HIPAA One® Question:** Is there a process to periodically review user accounts in this EMR/ePHI/PII system to ensure they belong to active, authorized workforce members that still need access to this EMR/ePHI/PII system (i.e. outside of any existing termination procedure including contractors or temporary users involved with testing or upgrading the ePHI software application)? **Included Comments:** User accounts are reviewed every 6 months by IT. HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** Tsystem2022Audit.PNG
Uintah Basin Healthcare Harmony - Health Data Archive 164.308(a)(3)(ii)(C), 164.310(a)(2)(iii), AC-2(g)(12) Workforce Security	**Section:** administrative **Specification:** Termination Procedures **HIPAA One® Question:** Is there a process to periodically review user accounts in this EMR/ePHI/PII system to ensure they belong to active, authorized workforce members that still need access to this EMR/ePHI/PII system (i.e. outside of any existing termination procedure including contractors or temporary users involved with testing or upgrading the ePHI software application)? **Included Comments:** semi-annual review by the ITS team. Updated Policy added - KV 09/28/21 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** UBH_Internal_Audit_H2_202 2.xlsx

Uintah Basin Healthcare Clarity 164.308(a)(3)(ii)(C), 164.310(a)(2)(iii), AC-2(g)(12) Workforce Security	**Section:** administrative **Specification:** Termination Procedures **HIPAA One® Question:** Is there a process to periodically review user accounts in this EMR/ePHI/PII system to ensure they belong to active, authorized workforce members that still need access to this EMR/ePHI/PII system (i.e. outside of any existing termination procedure including contractors or temporary users involved with testing or upgrading the ePHI software application)? **Included Comments:** The Technology department conducts a semi-annual review of all access accounts. The superuser reviews accounts at least semi-annually. Continues same, 10/4/2021 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:**
Uintah Basin Healthcare Point Click Care 164.308(a)(3)(ii)(C), 164.310(a)(2)(iii), AC-2(g)(12) Workforce Security	**Section:** administrative **Specification:** Termination Procedures **HIPAA One® Question:** Is there a process to periodically review user accounts in this EMR/ePHI/PII system to ensure they belong to active, authorized workforce members that still need access to this EMR/ePHI/PII system (i.e. outside of any existing termination procedure including contractors or temporary users involved with testing or upgrading the ePHI software application)? **Included Comments:** A supervisor goes thru the accounts at the beginning of every month and documents what/when she does. Verified KV 09/28/21 PM 2022 HIPAA One Analysis:11.3.2021 PM **Attachments:** UBH_Internal_Audit_H2_202 2.xlsx
Uintah Basin Healthcare Cerner 164.308(a)(3)(ii)(C), 164.310(a)(2)(iii), AC-2(g)(12) Workforce Security	**Section:** administrative **Specification:** Termination Procedures **HIPAA One® Question:** Is there a process to periodically review user accounts in this EMR/ePHI/PII system to ensure they belong to active, authorized workforce members that still need access to this EMR/ePHI/PII system (i.e. outside of any existing termination procedure including contractors or temporary users involved with testing or upgrading the ePHI software application)? **Included Comments:** We review user accounts and access every six months. HIPAA One Analysis: KV 10/05/21 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** UBH_Internal_Audit_H2_202 2 - Legacy Systems.pdf
Organization 164.308(a)(3)(ii)(C), AC-2(3) PS-4 Workforce Security	**Section:** administrative **Specification:** Termination Procedures **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP), and a formal process where HR notifies the EMR/ePHI/PII Administrator of termination/departures or other reasons to revoke EMR/ePHI/PII access? **Included Comments:** Badges are disabled by the HR assistant. Once an employee is terminated the HR assistant contacts IT. Added updated policy PM HIPAA One Analysis:11.3.2021 **Attachments:** Employment Termination Policy.docx ITS Employee Account Policy 4.2.pdf

Organization 164.308(a)(3)(ii)(C), PS-4 AC-2(h) Workforce Security	**Section:** administrative **Specification:** Termination Procedures **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) with a formal process where HR notifies IT of staff termination/departures or other reasons to revoke server/network access? **Included Comments:** HR submits a service request to our IT departments ticketing system notifying us of the termination. HR continues to notify us of terminations using our ticketing system. In most cases the accounts are terminated within 48 hours. If the user had access to sensitive data the account is disabled immediately as soon as we are notified. CZ Updated policy attached. ITS Employee Account Policy 4.1 Preston Marx HIPAA One Analysis:11.5.2021 PM **Attachments:** ITS Employee Account Policy 4.2.pdf
Organization 164.308(a)(4)(ii)(B), AC-2(b)(7) AC-3(7) PS-3 Information Access Management	**Section:** administrative **Specification:** Access Authorization **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place establishing and documenting who in the organization has elevated system permissions (i.e. System Administrators) and is authorized to add, edit or revoke user accounts in the EHR, RIS, PACS, Active Directory and any other ePHI systems? **Included Comments:** Added process to Account Policy. Revised and signed 10/21 PM HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** ITS Employee Account Policy 4.2.pdf
Organization 164.308(a)(5)(i), 164.308(a)(5)(ii)(C)-(D), AT-1 through AT-4 PM-13 PM-14 PS-6 Security Awareness Training	**Section:** administrative **Specification:** Security Awareness Training **HIPAA One® Question:** Does the organization have a HIPAA training Policy and Procedure (PnP) that outlines who needs to take training (by position or role), how they will be provided the training, is conducted AT LEAST annually and upon new-hires for employees, contractors and Business Associates? **Included Comments:** Employees complete HIPAA training at hire and annually online. Employees must pass the HIPAA test at 80%. The attachment shows training slides related to HIPAA Security. The Business Associate Agreement has an expectation that they are compliant with HIPAA which would include annual training for their staff. HIPAA One Analysis:11.3.2021 **Attachments:** HIPAA Security Rule Training.pdf Orientation OSHA CPR Policy.pdf

Organization 164.308(a)(5)(ii)(A), AT-2 PM-13 PM-14 SI-2(a) Security Awareness Training	**Section:** administrative **Specification:** Security Reminders **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place regarding a process to provide periodic HIPAA and Security-related reminders and communicate those reminders to the organization's staff? **Included Comments:** We require an annual HIPAA training of our employees and the same training upon hire. We have tried to assimilate refresher training in our department managers meetings. The ITS department speaks about HIPAA concerns at every department meeting. - 10/21 PM - Still in practice. HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** ITS Security Policy 1.3.pdf
Organization 164.308(a)(5)(ii)(B), CM-2(2) SI-2 (5) SI-7 Security Awareness Training	**Section:** administrative **Specification:** Protection from Malicious Software **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) with a process to maintain the most up-to-date firmware versions on your firewalls, wireless access points and Internet-facing devices (i.e. in the DMZ)? **Included Comments:** Moved to Meraki WLAN which keeps all infrastructure on latest OS. Also purchased Ordr to assist with keeping track of LAN hardware iOS versions. UBH Verified PM HIPAA One Analysis:11.3.2021 PM 2022 **Attachments:** ITS Network Management Policy 2.1.pdf Network Management Policy 2.2.pdf
Organization 164.308(a)(5)(ii)(B), CM-2(2) SI-3 Policies and Procedures	**Section:** administrative **Specification:** Protection from Malicious Software **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) and a process to maintain the most up-to-date security patches and O/S updates on servers, workstations, and other access devices? **Included Comments:** No Change. 11-8-2021 C Zobell We use WSUS for all workstations and notebooks now. all critical and security updates are patched every Wednesday. Update 12/01/2019:The new endpoint security procedure includes a policy on checking for updates on these devices. We recently migrated to a new private domain. Patches are not being applied as of right now in the new domain. The WSUS system has been created and is being tested now. It should be put into production within the next 30 days. CZ HIPAA One Analysis:11.5.2021 PM PM 2022 **Attachments:** Endpoint Security Procedure.pdf wsus.PNG

Organization 164.308(a)(5)(ii)(C), AC-2(g) AC-7 SI-5 Security Awareness Training	**Section:** administrative **Specification:** Log-in Monitoring (IT Manager) **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) requiring a process in which log-in attempts to the server/network environment are reviewed to identify potential brute-force (high number of failed login attempts) login attacks? **Included Comments:** We are using an application called AD Audit Plus to monitor failed login attempts. AD Audit Plus was purchased to catalog and report on login activity. Reports are reviewed by VP ITS weekly. HIPAA One Analysis:11.5.2021 PM **Attachments:** ITS Security Policy 1.3.pdf
Uintah Basin Healthcare Clarity 164.308(a)(5)(ii)(C), AC-7 SI-4 Security Awareness Training	**Section:** administrative **Specification:** Log-in Monitoring **HIPAA One® Question:** Do you have a process to review EMR/ePHI/PII system login attempts to identify potential brute-force (high number of failed login attempts) login attacks? **Included Comments:** Visonex/Clarity has this capability built-in and notifies in the event of a brute-force attack. Also multiple login attempts result in a locked out state that must be reversed by a superuser or Clarity after authentication. Clarity logs the login attempts within the client database. We also log unusual activity and notify support (the IP Attack emails) for review to determine if they are false positives based on the login records. If an event proved suspicious, we would notify the client /clinic that was impacted. Continues same, added PP from UGM 8/2021: 10/4/2021 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** HIPAA presentation UGM 2021.txt Password and Lockout requirements..docx
Organization 164.308(a)(5)(ii)(D) 164.310(d)(2)(ii) 164.312(a)(2)(iv), AC-19 IA-3 Security Awareness Training	**Section:** administrative **Specification:** Password Management **HIPAA One® Question:** Does the organization have some type of Mobile Device Management (MDM) platform such as Exchange, Office365 or other MDM platform AND require all workforce members to approve MDM policies on their devices before connecting? **Included Comments:** 11-9-2021 Added screenshot of gSuite tool. Showing requirements. We use GSuite for MDM regarding putting corporate email on a mobile devices. The device must have a locking mechanism enabled. Our policy is that non-UBH owned devices should not be connected to our network unless managed/registered with UBH Technology. HIPAA One Analysis:11.16.2021 PM PM 2022 **Attachments:** Endpoint Security Procedure.pdf gSuite_Enfore_PW_On_Mobil e_Device.PNG ITS Security Policy 1.3.pdf

Uintah Basin Healthcare Cerner 164.308(a)(5)(ii)(D), IA-5(c)(1) Security Awareness Training	**Section:** administrative **Specification:** Password Management **HIPAA One® Question:** Do you have HIPAA-compliant (i.e. Recommended for health care: minimum 8 characters, password complexity (i.e. special characters, numbers and upper or lower case, changed at least every 360 days and refusing last 3 remembered passwords OR passphrase which is a sentence that may be easier to remember than a very complex password) password management settings enabled in your EMR/ePHI/PII system and/or RIS/PACS? **Included Comments:** Passwords settings are: minimum of 8 characters, 2 out of the three following - uppercase, a number, or special character. expires every 90 days. Users are not allowed to use any part of their name in the password. KV 10/05 /21 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** Cerner password requirements.PNG Password requirements.PNG
Uintah Basin Healthcare Clarity 164.308(a)(5)(ii)(D), IA-5(c)(1) Security Awareness Training	**Section:** administrative **Specification:** Password Management **HIPAA One® Question:** Do you have HIPAA-compliant (i.e. Recommended for health care: minimum 8 characters, password complexity (i.e. special characters, numbers and upper or lower case, changed at least every 360 days and refusing last 3 remembered passwords OR passphrase which is a sentence that may be easier to remember than a very complex password) password management settings enabled in your EMR/ePHI/PII system and/or RIS/PACS? **Included Comments:** Continues same 10/4/2021 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** Password and Lockout requirements..docx
Uintah Basin Healthcare T-System 164.308(a)(5)(ii)(D), IA-5(c)(1) Security Awareness Training	**Section:** administrative **Specification:** Password Management **HIPAA One® Question:** Do you have HIPAA-compliant (i.e. Recommended for health care: minimum 8 characters, password complexity (i.e. special characters, numbers and upper or lower case, changed at least every 360 days and refusing last 3 remembered passwords OR passphrase which is a sentence that may be easier to remember than a very complex password) password management settings enabled in your EMR/ePHI/PII system and/or RIS/PACS? **Included Comments:** 10/21 - Policy ITS-6.1 Password Policy states that our passwords must follow the prescribed guidelines Preston Marx HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** ITS Password Policy 6.1.pdf passwordpolicyTSystem.PNG

Uintah Basin Healthcare Harmony - Health Data Archive 164.308(a)(5)(ii)(D), IA-5(c)(1) Security Awareness Training	**Section:** administrative **Specification:** Password Management **HIPAA One® Question:** Do you have HIPAA-compliant (i.e. Recommended for health care: minimum 8 characters, password complexity (i.e. special characters, numbers and upper or lower case, changed at least every 360 days and refusing last 3 remembered passwords OR passphrase which is a sentence that may be easier to remember than a very complex password) password management settings enabled in your EMR/ePHI/PII system and/or RIS/PACS? **Included Comments:** This is a legacy archival system that only a select few employees have access. This is for patient requests or historical retrieval. User access is managed by LDAP and security groups within our AD. KV 10/05/21 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** HarmonyAccess.PNG Password Policy 6.1.docx UBH Default Domain Policy PW Settings.PNG
Uintah Basin Healthcare Point Click Care 164.308(a)(5)(ii)(D), IA-5(c)(1) Security Awareness Training	**Section:** administrative **Specification:** Password Management **HIPAA One® Question:** Do you have HIPAA-compliant (i.e. Recommended for health care: minimum 8 characters, password complexity (i.e. special characters, numbers and upper or lower case, changed at least every 360 days and refusing last 3 remembered passwords OR passphrase which is a sentence that may be easier to remember than a very complex password) password management settings enabled in your EMR/ePHI/PII system and/or RIS/PACS? **Included Comments:** Verified KV 09/28/21 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** ITS Password Policy 6.1.pdf PasswordReqPCC.png PasswordReqPCC.png pw rules for PCC.PNG

Organization 164.308(a)(5)(ii)(D), IA-5(c)(1) Security Awareness Training	**Section:** administrative **Specification:** Password Management **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) requiring appropriate password security settings on the server/network environment (Active Directory or other User Account Lists) (i.e. Recommended for health care: long (over 20 characters) passphrase OR passwords with minimum 10 characters, password complexity, special characters, numbers and upper or lower case, changed every 180 days and remember last 3 passwords)? **Included Comments:** Uploaded screen shots of our default domain policy that controls the password policy for all domain accounts with the exception of the members of the IT department. I've also included screen shots of our Fine Grained Password Policy and the members of our facility that policy applies to (IT Staff). As you can see from the screen shot the Fine Grained Password Policy requires a minimum of 8 characters be used and the password must be a complex one meaning a mixture of upper and lower case letters as well as a number and a special character. A new password policy for our entire organization has been approved. As of 1/10/2017 all users accounts will be required to meet the standard mentioned. Our password policy meets these requirements. We don't deal with ePHI on mobile devices. CZ No change. 11-8/2021 C Zobell HIPAA One Analysis: 11.5.2021 PM **Attachments:** ITS Password Policy 6.1.pdf Password Policy.docx UBH Password Memo.pdf UBHpasswordGPO.PNG UBH_Default_Domain_Policy _PW_Settings.PNG
Organization 164.308(a)(6)(i), IR-1 through IR-8 Security Incident Procedures	**Section:** administrative **Specification:** Security Incident Procedures **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place to manage security related incidents, such as an Incident Response Plan process (e.g. what defines a security incident, who should be notified, containment, service restoration, lessons learned)? **Included Comments:** Reviewed/Updated policies 10/21 PM HIPAA One Analysis: 11.3.2021 PM PM 2022 **Attachments:** ITS Incident Response Policy 9.0 (1).pdf
Organization 164.308(a)(6)(ii), IR-4-8 PM-4 Security Incident Procedures	**Section:** administrative **Specification:** Response and Reporting **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place to document reported security incidents including activities taken to mitigate impact to the organization? **Included Comments:** There have been no reported security incidents to date. In the event a security incident is reported, we have an incident response plan and checklist to follow and will document the results. .11.3.2021 PM We had an cybersecurity incident in 2022. The results are still pending, but we have engaged a reputable cybersecurity partner to assist with the incident. They have cleared our network and system to resume activity. PM 2022 **Attachments:** ITS Incident Response Policy 9.0 (1).pdf

Organization 164.308(a)(6)(ii), IR-6 Security Incident Procedures	**Section:** administrative **Specification:** Response and Reporting **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) identifying the channels available for employees to report security incidents, potential HIPAA violations, non-compliance or general errors? **Included Comments:** Attachment shows contact number for reporting HIPAA violations is 435.722.4691 ext.6138. HIPAA One Analysis:11.3.2021 **Attachments:** ITS Incident Response Policy 9.0.pdf Non Retaliation for Complaints.pdf Receiving and Processing Complaints.pdf Workforce Privacy Agreement.docx
Organization 164.308(a)(7)(i), 164.312(a)(2)(ii)-(iii), CP-1 CP-2 CP-3 PE-10 through PE-18 Contingency Plan	**Section:** administrative **Specification:** Contingency Plan **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place to have an operational contingency plan that contains policies and procedures on how to respond to an emergency (i.e. that makes ePHI systems unavailable or damages them and provide access to ePHI during an emergency)? **Included Comments:** Reviewed/Updated policies 10/21 PM HIPAA One Analysis: 11.3.2021 PM PM 2022 **Attachments:** ITS Business Continuity Policy 7.1.pdf
Uintah Basin Healthcare 164.308(a)(7)(ii)(A), CA-2(c) CP-9 PL-1-2 Contingency Plan	**Section:** administrative **Specification:** Data Backup Plan **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) and Backup Plan (i.e. address backups, maintain retrievable exact copies of ePHI and tested restoration procedures)? **Included Comments:** Update 11.4.2019: All ePHI is now remote hosted. All backups are being managed by the respective vendors. Because of the way we're "grouped" together with other hospitals, sharing the EMR vendors resources we are unable to test restoration procedures. No Change. 11-8-2021 C Zobell HIPAA One Analysis:11.5.2021 PM **Attachments:** Backup Procedure.xlsx Backup Retention & Disaster Recovery Policy 10.0.pdf Management Response to SSAE-16 Report.pdf SOC 1 Type 2 Report - 2015 (Cerner).pdf SSAE-16 Bridge letter.pdf

Uintah Basin Healthcare - Vernal Campus 164.308(a)(7)(ii)(A), CA-2(c) CP-9 PL-1-2 Contingency Plan	**Section:** administrative **Specification:** Data Backup Plan **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) and Backup Plan (i.e. address backups, maintain retrievable exact copies of ePHI and tested restoration procedures)? **Included Comments:** Update 11.4.2019: All ePHI is now remote hosted. All backups are being managed by the respective vendors. Because of the way we're "grouped" together with other hospitals, sharing the EMR vendors resources we are unable to test restoration procedures. This has not changed. Still no EMR/ePHI/PII servers or databases exist at this location therefore backups are not needed here. CZ No Change. 11-8-2021 C Zobell HIPAA One Analysis:11.5.2021 PM **Attachments:** Backup Procedure.xlsx Backup Retention & Disaster Recovery Policy 10.0.pdf Backup Retention & Disaster Recovery Policy 10.0.pdf
Organization 164.308(a)(7)(ii)(B), CP-10 Contingency Plan	**Section:** administrative **Specification:** Disaster Recovery Plan **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place that includes a Disaster Recovery plan to restore critical system functionality and data in the event of an emergency? **Included Comments:** No Change. 11-8-2021 C Zobell The attached Business Continuity Policy describes our recovery plan. CZ HIPAA One Analysis:11.5.2021 PM **Attachments:** Backup Retention & Disaster Recovery Policy 10.0.pdf ITS Business Continuity Policy 7.1.pdf
Organization 164.308(a)(7)(ii)(C), CP-1 CP-2(4) CP-11 Contingency Plan	**Section:** administrative **Specification:** Emergency Mode Operation Plan **HIPAA One® Question:** Does the organization have a business continuity Policy and Procedure (PnP) developed for your organization to continue critical business operations and protection of ePHI during an emergency? **Included Comments:** Reviewed/Updated policies 10/21 PM HIPAA One Analysis: 11.3.2021 PM PM 2022 **Attachments:** ITS Business Continuity Policy 7.1.pdf
Organization 164.308(a)(7)(ii)(D), CA-2(c) CP-4 Contingency Plan	**Section:** administrative **Specification:** Testing and Revision Procedures **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place to periodically test the business continuity scenarios for your organization and for periodic testing of these contingency plans? **Included Comments:** Moving to Yes as we have an annual imposed downtime with the change to daylight savings. The systems are down for 2-3 hours which gives a good test of downtime procedures. Reviewed/Updated policies 10/21 PM HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** ITS Business Continuity Policy 7.1.pdf

Organization 164.308(a)(7)(ii)(E), CP-2(8) CP-10 PL-1-2 PM-8 RA-2(a) RA-9 Contingency Plan	**Section:** administrative **Specification:** Applications and Data Criticality Analysis **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) that requires prioritization of the organization's servers and data based on criticality and required restore point objectives? **Included Comments:** No Change. 11-8-2021 C Zobell All of our critical systems are given level of importance. The level the system falls in will determine the backup frequency and number of retention days. CZ HIPAA One Analysis: 11.5.2021 PM **Attachments:** Backup Procedure.xlsx Backup Retention & Disaster Recovery Policy 10.0.pdf UBH_Server_Backup_Strateg y.PNG
Organization 164.308(a)(8), CA-1-2 Evaluation	**Section:** administrative **Specification:** Evaluation **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place to perform a periodic technical and non-technical security evaluation after environmental or operational changes affecting the security of ePHI (e.g. staff changes, application upgrades, data migrations, backups, mobile-device and other access devices) with approved change management procedures requiring approvals for changes to operating systems, servers, network(s), application(s), and security devices? **Included Comments:** Changes to the EMR are put in a non-production environment first and tested by members of the informatics team. Once the update is put in production, AAA parameters are reviewed. Reviewed/Updated policies 10 /21 PM HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** ITS Business Continuity Policy 7.1.pdf
Organization 164.308(b)(1), 164.308(b)(3), AC-3 (9) AC-20 CA-3 PS-6 PS-7(a) Business Associate Contracts and Other Arrangements -- Written Contract or Other Arrangement	**Section:** administrative **Specification:** Written Contract **HIPAA One® Question:** Do you have a report showing all the vendors that have signed the BAA, accessible to those staff that need to view it? **Included Comments:** https://drive.google.com/drive/u/0/folders /107BkGyweaMaofWcjsafMBbeLUuRKa4E9 Preston Marx **Attachments:** HIPAA One artifact default.pdf

Organization 164.308(b)(3), AC-20 AC-21 CA-3 PS-6 SA-1 Business Associate Contracts and Other Arrangements	**Section:** administrative **Specification:** Written Contract **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place where all the vendors and subcontractors which may receive, occasionally view (e.g. remote IT support) or otherwise exchange the organization's ePHI have a signed a Business Associate Agreement? **Included Comments:** 10/21 - All BAA's were put in a shared drive accessible by compliance committee. https://drive.google.com/drive/u/0/folders /107BkGyweaMaofWcjsafMBbeLUuRKa4E9 Preston Marx HIPAA One Analysis: 11.16.2021 PM PM 2022 **Attachments:** Business Associates Agreement.doc Disclosing Protected Health Information to Business Associates .pdf How to Determine if a BAA is needed.docx HP-27 Disclosing PHI to Business Associates.doc
Uintah Basin Healthcare 164.310(a)(1), PE-1-3 PE-18 Facility Access Controls	**Section:** physical **Specification:** Facility Access Controls **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) that governs facility access controls limiting physical access to where the servers and/or network equipment and/or computing devices accessing ePHI are housed? (e.g. are there locks on the door to the server/network room(s) and to areas with computers that access ePHI)? **Included Comments:** This door has an electronic mag lock which is locked 24/7 and is only accessible by staff who have access with a Wiegand/Proximity card or key fob. Added Date and approval section to facilities policy. Signed. PM 11/15 /2021 PM 2022 **Attachments:** Copy of IT Server Room Access 2017.xls ENG Physical Facilities Access Policy.pdf ITS Security Policy 1.3.pdf ITS Security Policy 1.4.pdf Physical Facility Access Policy.docx UBH Server room door.jpg
Uintah Basin Healthcare 164.310(a)(2)(i), CP-2 CP-10 AC-3 PE-17 PE-18 Facility Access Controls	**Section:** physical **Specification:** Contingency Operations **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place for facility access so IT personnel can access the Data Center / Main Data Facility for the purposes of disaster recovery or emergency mode operations? **Included Comments:** No Change. 11-8-2021 C Zobell Update 11.4.2019: All IT staff members still have badge access to our data center. It is 24/7 access that is audit able. CZ HIPAA One Analysis:11.5.2021 PM PM 2022 **Attachments:** ITS Security Policy 1.3.pdf

Uintah Basin Healthcare 164.310(a)(2)(ii), PE-1-7 Facility Access Controls	**Section:** physical **Specification:** Facility Security Plan **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) to secure physical access into the organization's buildings and safeguard computer equipment from unauthorized physical access, tampering and theft? **Included Comments:** Added Date and approval section to facilities policy. Signed. PM 11/15/2021 PM 2022 **Attachments:** Elevator requires card access.JPG ENG Physical Facilities Access Policy.pdf Physical Facility Access Policy.docx
Uintah Basin Healthcare - Vernal Campus 164.310(a)(2)(ii), PE-1-7 Facility Access Controls	**Section:** physical **Specification:** Facility Security Plan **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) to secure physical access into the organization's buildings and safeguard computer equipment from unauthorized physical access, tampering and theft? **Included Comments:** Added Date and approval section to facilities policy. Signed. PM 11/15/2021 PM 2022 **Attachments:** ENG Physical Facilities Access Policy.pdf Physical Facility Access Policy.docx
Organization 164.310(b), AC-4 AC-11 AC-16 Workstation Use	**Section:** physical **Specification:** Workstation Use **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place with some type of End-User Acceptable Use contract that includes appropriate use with specific guidelines for each class of workstation in place for your organization? **Included Comments:** Reviewed/Updated policies 10/21 PM HIPAA One Analysis: 11.3.2021 PM PM 2022 **Attachments:** ITS Acceptable Use Policy 3.1.pdf
Uintah Basin Healthcare - Vernal Campus 164.310(c), MP-2 PE-1-3 PE-6 Workstation Security	**Section:** physical **Specification:** Workstation Security **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place for ensuring workstations that have access to ePHI systems are physically secure from unauthorized access (i.e. not facing patient-waiting areas, not accessible via public areas, behind locked doors, etc.)? **Included Comments:** Added Date and approval section to facilities policy. Signed. PM 11/15/2021 PM 2022 **Attachments:** CONFIDENTIALITY.docx ITS Security Policy 1.3.pdf ITS Security Policy 1.4.pdf Vernal Clinic patient hallway.jpg Vernal Lab reception desk.jpg

Uintah Basin Healthcare 164.310(c), MP-2 PE-1-3 PE-6 Workstation Security	**Section:** physical **Specification:** Workstation Security **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place for ensuring workstations that have access to ePHI systems are physically secure from unauthorized access (i.e. not facing patient-waiting areas, not accessible via public areas, behind locked doors, etc.)? **Included Comments:** HIPAA One Analysis: 11.3.2021 PM 2022 **Attachments:** CONFIDENTIALITY.docx ENG Physical Facilities Access Policy.pdf ITS Security Policy 1.3.pdf ITS Security Policy 1.4.pdf Physical Facility Access Policy.docx
Organization 164.310(d)(1), 164.310(d)(2)(iii), CM-10 MP-1 through MP-7 Device and Media Controls	**Section:** physical **Specification:** Accountability **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place to provide guidelines or rules to staff regarding the removal, download or storage of ePHI stored on hard drives or removable media (i.e. thumb drive, DVD, smartphones, etc.)? **Included Comments:** Reviewed/Updated policies 10/21 PM HIPAA One Analysis: 11.3.2021 PM PM 2022 **Attachments:** ITS Acceptable Use Policy 3.1.pdf
Organization 164.310(d)(1), 164.310(d)(2)(iii), CM-8(4) MP-2 Device and Media Controls	**Section:** physical **Specification:** Accountability **HIPAA One® Question:** Who is the individual assigned the responsibility to maintain a record of the movement of hardware and electronic media (i.e. Desktops, laptops, tablets, USB drives, backup media, DVD, CD, smartphones, and PDAs.) containing ePHI? **Included Comments:** Jennifer Aumiller Jennifer_Aumiller@ubh.org (435) 725-2050 xt 1713 **Attachments:**
Organization 164.312(a)(1), 164.308(a)(4)(ii)(C), 164.308(a)(4)(i), 164.312(c)(1)-(2), AC-2(11) AC-3(7) AC-6 Workforce Security, Information Access Management	**Section:** administrative **Specification:** Access Establishment and Modification **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place to review user accounts in your organization, and software-applications to ensure their access levels (including read, modify or delete records to avoid improper alteration or destruction) match their job description or function, including minimum necessary per the HIPAA Privacy Rule? **Included Comments:** The ITS department does a semi-annual review of access to systems, and it is included in the Employee Account Policy. 10/21 PM HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** ITS Security Policy 1.3.pdf

Organization 164.312(a)(1), 164.308(a)(3)(ii)(C), PS-4 Workforce Security	**Section:** administrative **Specification:** Termination Procedures **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) along with some type of checklist to recover employee access control devices (ID badges, keys, etc.), logon accounts, computers, smartphones and delivery of any data/information from workforce members when employment ends? **Included Comments:** Employment Separation Form. Employment Termination Policy HIPAA One Analysis:11.3.2021 **Attachments:** EMP SEPARATION FORM.pdf Employment Termination Policy.docx ITS Employee Account Policy 4.2.pdf
Uintah Basin Healthcare Point Click Care 164.312(a)(2)(i), 170.314(d)(1)(i), AC-3(7) AU-2(14) IA-2 Access Control	**Section:** technical **Specification:** Unique User Identification (EMR/ePHI/PII Administrator) **HIPAA One® Question:** Does each individual in the organization that has access to the EMR/ePHI/PII program have a unique user ID? **Included Comments:** Verified KV 09/28/21 User access was reviewed and deemed appropriate. PM 12/03/2020 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** ITS Employee Account Policy 4.2.pdf PCCUsernames.png
Uintah Basin Healthcare Clarity 164.312(a)(2)(i), 170.314(d)(1)(i), AC-3(7) AU-2(14) IA-2 Access Control	**Section:** technical **Specification:** Unique User Identification (EMR/ePHI/PII Administrator) **HIPAA One® Question:** Does each individual in the organization that has access to the EMR/ePHI/PII program have a unique user ID? **Included Comments:** Clarity does not allow more than one individual to utilize the same login account ID. Continues same, 10/4/2021 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** unique user list.docx
Uintah Basin Healthcare Cerner 164.312(a)(2)(i), 170.314(d)(1)(i), AC-3(7) AU-2(14) IA-2 Access Control	**Section:** technical **Specification:** Unique User Identification (EMR/ePHI/PII Administrator) **HIPAA One® Question:** Does each individual in the organization that has access to the EMR/ePHI/PII program have a unique user ID? **Included Comments:** We use the naming convention of firstname_lastname for users names, in the very rare occasion that we have users with the same first name we will add a middle name or a number 2 to their username. HIPAA One Analysis: KV 10/05/21 PM 2022 **Attachments:** 421838288.xlsx HNA Tucker.PNG ITS Employee Account Policy 4.2.pdf

Uintah Basin Healthcare T-System 164.312(a)(2)(i), 170.314(d)(1)(i), AC-3(7) AU-2(14) IA-2 Access Control	**Section:** technical **Specification:** Unique User Identification (EMR/ePHI/PII Administrator) **HIPAA One® Question:** Does each individual in the organization that has access to the EMR/ePHI/PII program have a unique user ID? **Included Comments:** There is one generic tracking account (.screensaver) for displaying which rooms patients are in. This account is view-only and cannot be used to modify patient records. HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** ITS Employee Account Policy 4.2.pdf Tsystem log ons.docx
Uintah Basin Healthcare Harmony - Health Data Archive 164.312(a)(2)(i), 170.314(d)(1)(i), AC-3(7) AU-2(14) IA-2 Access Control	**Section:** technical **Specification:** Unique User Identification (EMR/ePHI/PII Administrator) **HIPAA One® Question:** Does each individual in the organization that has access to the EMR/ePHI/PII program have a unique user ID? **Included Comments:** Attachment shows a listing of unique user ID's. KV 10/05/21 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** CPSIClinical.PNG CPSIFinancials.PNG CPSI_HR.PNG nextgenclinical1.PNG nextgenclinical2.PNG nextgenfinancial.PNG
Uintah Basin Healthcare Cerner 164.312(a)(2)(ii), 170.314(d)(6), AC-2 AC-3(10)-(11) Access Control	**Section:** technical **Specification:** Emergency Access Procedure **HIPAA One® Question:** Is your EMR/ePHI/PII package configured to allow additional privacy permissions (e.g. for high-profile patients) to patient information AND configured emergency access (i.e. break the glass) so workforce staff may access restricted patients in the EMR/ePHI/PII without calling an administrator? **Included Comments:** Whenever you access a patient chart you have to choose your relationship to the patient. If it is an emergency you can choose Emergency Access and then choose an override reason. If other is chosen then the user must type in the reason. KV 10/05/21 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** Break The Glass.PNG Confidentiality Level.PNG

Uintah Basin Healthcare Clarity 164.312(a)(2)(ii), 170.314(d)(6), CP-2(7) CP-9 PE-11 Access Control	**Section:** technical **Specification:** Emergency Access Procedure **HIPAA One® Question:** In the event of a power-outage emergency, Is your EMR /ePHI/PII package connected to an Uninterruptible Power Supply (UPS), power-generator, and/or in a separate data center so users may continue to access the EMR/ePHI/PII package during that power outage? **Included Comments:** This is a web-based application and may be accessed. It is hosted remotely and has redundant power supplies and hosted sites. In the event of a local power outage it can be accessed via individual laptop computers with battery backup capability. There is also a generator that provides backup power. The Clarity system can also be accessed via cell phone or tablet with internet access. The facility backup generator goes through backup testing weekly, with a load test at least quarterly. Continues, Has demonstrated capability during the year with several outages. 10/4/2021 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:**
Uintah Basin Healthcare Point Click Care 164.312(a)(2)(ii), 170.314(d)(6), CP-2(7) CP-9 PE-11 Access Control	**Section:** technical **Specification:** Emergency Access Procedure **HIPAA One® Question:** In the event of a power-outage emergency, Is your EMR /ePHI/PII package connected to an Uninterruptible Power Supply (UPS), power-generator, and/or in a separate data center so users may continue to access the EMR/ePHI/PII package during that power outage? **Included Comments:** This is a web-based application, so a local power-outage will not affect this EMR's availability. Verified KV 09/28/21 PM 2022 HIPAA One Analysis:11.3.2021 PM **Attachments:**
Uintah Basin Healthcare T-System 164.312(a)(2)(ii), 170.314(d)(6), CP-2(7) CP-9 PE-11 Access Control	**Section:** technical **Specification:** Emergency Access Procedure **HIPAA One® Question:** In the event of a power-outage emergency, Is your EMR /ePHI/PII package connected to an Uninterruptible Power Supply (UPS), power-generator, and/or in a separate data center so users may continue to access the EMR/ePHI/PII package during that power outage? **Included Comments:** This solution is remote hosted by the vendor. This application is housed in a data center that is climate controlled and has UPS power in place. Our access to the solution requires a network connection at our site; which is also UPS protected. HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:**

Uintah Basin Healthcare Harmony - Health Data Archive 164.312(a)(2)(ii), 170.314(d)(6), CP-2(7) CP-9 PE-11 Access Control	**Section:** technical **Specification:** Emergency Access Procedure **HIPAA One® Question:** In the event of a power-outage emergency, Is your EMR /ePHI/PII package connected to an Uninterruptible Power Supply (UPS), power-generator, and/or in a separate data center so users may continue to access the EMR/ePHI/PII package during that power outage? **Included Comments:** the system is remote hosted by the vendor and it protected by UPS. An internet connection is the only thing required from our local end. KV 10 /05/21 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:**
Uintah Basin Healthcare Harmony - Health Data Archive 164.312(a)(2)(iii), 170.314(d)(5) , AC-2(5) AC-11-12 Access Control	**Section:** technical **Specification:** Automatic Logoff **HIPAA One® Question:** Do you have an EMR/ePHI/PII or PACS session-timer mechanism in place to logoff or lock workstations after a period of inactivity? **Included Comments:** session timeout is configured to logoff after 10 minutes of inactivity. KV 10/05/21 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** UBH Inactivity TimeOut Group Policy (1).PNG
Uintah Basin Healthcare Cerner 164.312(a)(2)(iii), 170.314(d)(5) , AC-2(5) AC-11-12 Access Control	**Section:** technical **Specification:** Automatic Logoff **HIPAA One® Question:** Do you have an EMR/ePHI/PII or PACS session-timer mechanism in place to logoff or lock workstations after a period of inactivity? **Included Comments:** Cerner is configured to logoff after 30 minutes of inactivity. KV 10/05/21 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** Cerner Session logout.PNG
Uintah Basin Healthcare T-System 164.312(a)(2)(iii), 170.314(d)(5) , AC-2(5) AC-11-12 Access Control	**Section:** technical **Specification:** Automatic Logoff **HIPAA One® Question:** Do you have an EMR/ePHI/PII or PACS session-timer mechanism in place to logoff or lock workstations after a period of inactivity? **Included Comments:** Attachment shows that Terminal Services has a session timeout setting of 3 hours. HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** T-System Time out.JPG
Uintah Basin Healthcare Clarity 164.312(a)(2)(iii), 170.314(d)(5) , AC-2(5) AC-11-12 Access Control	**Section:** technical **Specification:** Automatic Logoff **HIPAA One® Question:** Do you have an EMR/ePHI/PII or PACS session-timer mechanism in place to logoff or lock workstations after a period of inactivity? **Included Comments:** 45min Continues same, 10/4/2021 HIPAA One Analysis: 11.3.2021 PM PM 2022 **Attachments:** Password and Lockout requirements..docx

Uintah Basin Healthcare Point Click Care 164.312(a)(2)(iii), 170.314(d)(5) , AC-2(5) AC-11-12 Access Control	**Section:** technical **Specification:** Automatic Logoff **HIPAA One® Question:** Do you have an EMR/ePHI/PII or PACS session-timer mechanism in place to logoff or lock workstations after a period of inactivity? **Included Comments:** It is set to 30 min. HIPAA One Analysis: Verified KV 09/28 /21 PM 2022 **Attachments:** PCCTimeout.png
Organization 164.312(a)(2)(iii), AC-12 SC-10 Access Control	**Section:** technical **Specification:** Automatic Logoff **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) and session-timer mechanism in place to logoff or lock workstations after a period of inactivity? **Included Comments:** No Change. 11-8-2021 C Zobell I most areas we do have some sort of session timer but not all. The session timer is used in all hospital areas, administration and IT but not in clinic areas. The session timer is a mix between an Imprivata time out on those machines that are Imprivata enabled and group policy for those machines that are not Imprivata enabled. We enforce a 30 minute inactivity screen lock on all of our domain computers. Imprivata users screens will lock after 10 minutes of inactivity. CZ HIPAA One Analysis:11.5.2021 PM PM 2022 **Attachments:** Endpoint Security Procedure.pdf UBH VDI end-user IGEL 1.jpg UBH VDI end-user IGEL 2.jpg UBH_Inactivity_TimeOut_Gr oup_Policy.PNG

Uintah Basin Healthcare 164.312(a)(2)(iv), AC-19(4)-(5) SC-7 SC-13 SC-28(1) Access Control	**Section:** technical **Specification:** Encryption and Decryption **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) including evidence of strong, full-disk encryption enabled for any data at rest (i.e. servers, laptops, mobile devices, multi-function printers, backup media, and USB keys)? **Included Comments:** Update: This is still the same, all mobile devices or machines in public areas that are at risk for theft are encrypted. USB keys are only allowed on devices that have been approved by a manager for a business purpose. All laptops are encrypted using Sophos SafeGuard. Computers that are in public locations that are at risk of theft are also encrypted using Sophos SafeGuard. USB ports are disabled on all computers unless a department manager or VP requests access for a specific user to have access to mass storage devices. Users must be members of a security group within Active Directory to be able to use mass storage devices. Members of this security group are meant to be audited regularly by department managers and/or VP's to ensure only those users with a business purpose are being given access to mass storage devices. MFP's are using their built in encryption. CZ 11-9-2021 The second paragraph in the security section of the ITS Acceptable Use Policy 3.1 document states that any terminal that requires PHI to be stored on it must be encrypted. It is a standard practice at UBH to encrypt all laptops. This is done when the machine is deployed. It it tracked by Jennifer Aumiller as a part of our asset inventory. CZ HIPAA One Analysis: Marked No so an updated ITS Acceptable Use Policy 3.1 can be provided. The attached ITS Acceptable Use Policy 3.1 is showing a version of 2016. PM 11-5-2021 PM 2022 Policy attached. **Attachments:** ITS Acceptable Use Policy 3.1.pdf SafeGuard Screen Shot for HIPPAOne.PNG UBH Laptop Encryption current.jpg UBH MFP Encrypted.jpg

Uintah Basin Healthcare - Vernal Campus 164.312(a)(2)(iv), AC-19(4)-(5) SC-7 SC-13 SC-28(1) Access Control	**Section:** technical **Specification:** Encryption and Decryption **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) including evidence of strong, full-disk encryption enabled for any data at rest (i.e. servers, laptops, mobile devices, multi-function printers, backup media, and USB keys)? **Included Comments:** Update 12/01/2019:The new endpoint security procedure includes a policy on checking for encryption on these devices. Update 11.4.2019: This is still the same, all mobile devices or machines in public areas that are at risk for theft are encrypted. USB keys are only allowed on devices that have been approved by a manager for a business purpose. All Mobile devices are now encrypted. USB keys are not allowed without manager approval. All laptops are encrypted using Sophos SafeGuard. Computers that are in public locations that are at risk of theft are also encrypted using Sophos SafeGuard. USB ports are disabled on all computers unless a department manager or VP requests access for a specific user to have access to mass storage devices. Users must be members of a security group within Active Directory to be able to use mass storage devices. Members of this security group are meant to be audited regularly by department managers and /or VP's to ensure only those users with a business purpose are being given access to mass storage devices. MFP's are using their built in encryption. CZ HIPAA One Analysis: Marked No so an updated ITS Acceptable Use Policy 3.1 can be provided. The attached ITS Acceptable Use Policy 3.1 is showing a version of 2016. PM 11-5-2021 11-9-2021 The second paragraph in the security section of the ITS Acceptable Use Policy 3.1 document states that any terminal that requires PHI to be stored on it must be encrypted. It is a standard practice at UBH to encrypt all laptops. This is done when the machine is deployed. It it tracked by Jennifer Aumiller as a part of our asset inventory. CZ PM 2022 **Attachments:** Aficio 301 MFP not encrypted 2.jpg ITS Acceptable Use Policy 3.1.pdf MFP with encryption icon 2.jpg SafeGuard Screen Shot for HIPPAOne.PNG
Uintah Basin Healthcare Clarity 164.312(b), 170.314(d)(2)-(3), 170.314(d)(7), 170.314(d)(9), AC-2 (g) AC-9 AU-2(d) Audit Controls	**Section:** technical **Specification:** Audit Controls **HIPAA One® Question:** ePHI System configuration check: Is your EMR/ePHI/PII (i. e. application housing ePHI) package configured with the following (All features must be ON to answer YES): system logging status, record all ePHI accesses, end-user encryption OR not storing ePHI on end-user devices, audit-log protection (i.e. changed or deleted not allowed), detection if the audit log is altered and <optional> description of disclosures recorded for treatment, payment, and healthcare operations? **Included Comments:** Continues same, 10/4/2021 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** audit log.docx

Uintah Basin Healthcare Cerner 164.312(b), 170.314(d)(2)-(3), 170.314(d)(7), 170.314(d)(9), AC-2 (g) AC-9 AU-2(d) Audit Controls	**Section:** technical **Specification:** Audit Controls **HIPAA One® Question:** ePHI System configuration check: Is your EMR/ePHI/PII (i.e. application housing ePHI) package configured with the following (All features must be ON to answer YES): system logging status, record all ePHI accesses, end-user encryption OR not storing ePHI on end-user devices, audit-log protection (i.e. changed or deleted not allowed), detection if the audit log is altered and <optional> description of disclosures recorded for treatment, payment, and healthcare operations? **Included Comments:** Screen captures of audit logs requested. KV 10/05/21 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** P2Sentinel Screenshot.PNG
Uintah Basin Healthcare T-System 164.312(b), 170.314(d)(2)-(3), 170.314(d)(7), 170.314(d)(9), AC-2 (g) AC-9 AU-2(d) Audit Controls	**Section:** technical **Specification:** Audit Controls **HIPAA One® Question:** ePHI System configuration check: Is your EMR/ePHI/PII (i.e. application housing ePHI) package configured with the following (All features must be ON to answer YES): system logging status, record all ePHI accesses, end-user encryption OR not storing ePHI on end-user devices, audit-log protection (i.e. changed or deleted not allowed), detection if the audit log is altered and <optional> description of disclosures recorded for treatment, payment, and healthcare operations? **Included Comments:** See attached. Verified: PM 10/21 HIPAA One Analysis: 11.3.2021 PM PM 2022 **Attachments:** T-System access.PNG TSystemAccounts - Sheet2.pdf
Organization 164.312(b), MP-5 PE-20 SA-10-14 SI-7-8 Audit Controls	**Section:** technical **Specification:** Audit Controls **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) establishing a content-aware solution (Data Classification and Data Loss Prevention) in place to discover, monitor, block, and safeguard electronic Protected Health Information (ePHI) during transit and at rest across network, storage, and endpoint systems? **Included Comments:** we have this capability in GSuite, but not locally. 01-14-2020 - DLP for SSN and Credit Cards enabled on UBH email system Preston Marx HIPAA One Analysis:11.3.2021 **Attachments:** DLP.PNG Network Management Policy 2.2.pdf

Uintah Basin Healthcare Point Click Care 164.312(c)(1)-(2), 170.314(d)(1)(ii), PM-23 SI-7 Integrity	**Section:** technical **Specification:** Mechanism to Authenticate Electronic Protected Health Information **HIPAA One® Question:** Is the EMR/ePHI/PII software configured so that only authorized individuals can EDIT and DELETE ePHI/PII (i.e. through security roles, security groups or other tiered access levels)? **Included Comments:** Modules are set up with certain ones only being able to modify. Monthly Audit is done on this also. HIPAA One Analysis: Verified KV 09/28 /21 PM 2022 User access was reviewed and deemed appropriate. PM 12/03/2020 **Attachments:** SecurityGroupPCC.JPG
Uintah Basin Healthcare Harmony - Health Data Archive 164.312(c)(1)-(2), 170.314(d)(1)(ii), PM-23 SI-7 Integrity	**Section:** technical **Specification:** Mechanism to Authenticate Electronic Protected Health Information **HIPAA One® Question:** Is the EMR/ePHI/PII software configured so that only authorized individuals can EDIT and DELETE ePHI/PII (i.e. through security roles, security groups or other tiered access levels)? **Included Comments:** Security groups are configured so only authorized individuals can edit ePHI. KV 10/05/21 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** harmony_access_groups.PNG
Uintah Basin Healthcare Cerner 164.312(c)(1)-(2), 170.314(d)(1)(ii), PM-23 SI-7 Integrity	**Section:** technical **Specification:** Mechanism to Authenticate Electronic Protected Health Information **HIPAA One® Question:** Is the EMR/ePHI/PII software configured so that only authorized individuals can EDIT and DELETE ePHI/PII (i.e. through security roles, security groups or other tiered access levels)? **Included Comments:** The CAH medical record/PC view only does not have access to edit anything in the patient's record. The CAH RN position does have access to edit the chart. KV 10/05/21 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** CAH medical records.PNG CAH RN.PNG ITS Employee Account Policy 4.2.pdf
Uintah Basin Healthcare Clarity 164.312(c)(1)-(2), 170.314(d)(1)(ii), PM-23 SI-7 Integrity	**Section:** technical **Specification:** Mechanism to Authenticate Electronic Protected Health Information **HIPAA One® Question:** Is the EMR/ePHI/PII software configured so that only authorized individuals can EDIT and DELETE ePHI/PII (i.e. through security roles, security groups or other tiered access levels)? **Included Comments:** See attached. Continues same. Security roles are in place. 10/4/2021 Continues same, 10/4/2021 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** AdvancedMD - HIPAA One 10-5-17 (4).docx

Uintah Basin Healthcare T-System 164.312(c)(1)-(2), 170.314(d)(1)(ii), PM-23 SI-7 Integrity	**Section:** technical **Specification:** Mechanism to Authenticate Electronic Protected Health Information **HIPAA One® Question:** Is the EMR/ePHI/PII software configured so that only authorized individuals can EDIT and DELETE ePHI/PII (i.e. through security roles, security groups or other tiered access levels)? **Included Comments:** Attachment shows various security groups and their ability to edit or not edit ePHI. HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** t system position guide.docx TSystemUsers2020.PNG
Uintah Basin Healthcare Point Click Care 164.312(d), 170.315(d)(13), IA-2 Person or Entity Authentication	**Section:** technical **Specification:** Audit Controls **HIPAA One® Question:** Has there been any effort to determine if the login process for this application is appropriate considering the data's level of sensitivity and ensuring the person logging in is who they say they are? **Included Comments:** User ID and Password Requirements have been changed. Jennifer Aumiller KV 09/28/21 PM 2022 **Attachments:** ITS Password Policy 6.1.pdf PasswordReqPCC.png
Uintah Basin Healthcare Harmony - Health Data Archive 164.312(d), 170.315(d)(13), IA-2 Person or Entity Authentication	**Section:** technical **Specification:** Audit Controls **HIPAA One® Question:** Has there been any effort to determine if the login process for this application is appropriate considering the data's level of sensitivity and ensuring the person logging in is who they say they are? **Included Comments:** userID and passwords that comply with our AD policy. complex, changed every 90 days. KV 10/05/21 HIPAA One Analysis:11.3.2021 PM LDAP password policy changed to 15 characters. only expires upon suspicion. PM 2022 **Attachments:** ITS Password Policy 6.1.pdf
Uintah Basin Healthcare Clarity 164.312(d), 170.315(d)(13), IA-2 Person or Entity Authentication	**Section:** technical **Specification:** Audit Controls **HIPAA One® Question:** Has there been any effort to determine if the login process for this application is appropriate considering the data's level of sensitivity and ensuring the person logging in is who they say they are? **Included Comments:** username and password User name is unique to entire Visonex system. Also Dialysis department has gone to the VDI system requiring use of badges or facility user name and password use to access the EMR. Also, now using VDI technology and badge into computer system technology, 10/4/2021 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** HIPAA One verification document.docx

Uintah Basin Healthcare Cerner 164.312(d), 170.315(d)(13), IA-2 Person or Entity Authentication	**Section:** technical **Specification:** Audit Controls **HIPAA One® Question:** Has there been any effort to determine if the login process for this application is appropriate considering the data's level of sensitivity and ensuring the person logging in is who they say they are? **Included Comments:** User ID and Password. We have also incorporated MFA with the use of Imprivata. It uses a corporate issued RFID badge plus a PIN to access the system. KV 10/05/21 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** badge reader settings.PNG
Uintah Basin Healthcare 164.312(e)(1)-(2)(i), 170.314(d)(8), AC-4 MP-5 PM-23 SC-8 SC-13 SI-3 SI-7 Integrity	**Section:** technical **Specification:** Integrity Controls **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) to ensure ePHI being transmitted is not altered during transmission across public networks (SHA256 or greater hashing algorithm) when accessing ePHI systems? **Included Comments:** Network management policy updated. Also Acceptable use policy states that access should only be from a secure network. Policy reviewed in 2021. PM PM 2022 **Attachments:** ITS Acceptable Use Policy 3.1.pdf Network Management Policy 2.2.pdf
Uintah Basin Healthcare 164.312(e)(1)-(2)(ii), AC-4 AC-17 (2) PM-23 SC-7-8 SC-11 SC-13 SI-3 SI-7 Integrity	**Section:** technical **Specification:** Encryption **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) to ensure the encryption level for electronic transmission of ePHI is at least: 3DES, AES, or EES, or Asymmetric keys: RSA PKCS #1, employing 128-bit ciphers or larger to ensure all ePHI being transmitted is sufficiently encrypted during transmission (i.e. TLS access to EMR/ePHI/PII, VPN tunnels, etc.)? **Included Comments:** Updated Network management policy to contain this info. UBH Verified PM HIPAA One Analysis:11.3.2021 **Attachments:** Network Management Policy 2.2.pdf
Uintah Basin Healthcare - Vernal Campus 164.312(e)(1)-(2)(ii), AC-4 AC-17 (2) PM-23 SC-7-8 SC-11 SC-13 SI-3 SI-7 Integrity	**Section:** technical **Specification:** Encryption **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) to ensure the encryption level for electronic transmission of ePHI is at least: 3DES, AES, or EES, or Asymmetric keys: RSA PKCS #1, employing 128-bit ciphers or larger to ensure all ePHI being transmitted is sufficiently encrypted during transmission (i.e. TLS access to EMR/ePHI/PII, VPN tunnels, etc.)? **Included Comments:** Updated Network management policy to contain this info. UBH Verified PM HIPAA One Analysis:11.3.2021 **Attachments:** Network Management Policy 2.2.pdf

Uintah Basin Healthcare - Vernal Campus 164.312(e)(1)-(2)(ii), SC-8(3) SC-11-13 SC-40 SI-4(14) SI-8 AC-18 (1) Transmission Security	**Section:** technical **Specification:** Encryption - Wireless Networks **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) for wireless networks and wireless encryption (Must be: AES, 3DES or EES)? **Included Comments:** Network Management policy attached. Uses 802.1x w /Radius authentication The UBH Private network both wired and wireless is secure and encrypted and is the medium from which to access PHI systems. UBH Guest Wireless and other unsecure networks should not be used for PHI access. See attached policy. **Attachments:** Network Management Policy 2.2.pdf UBH WiFi 2 encrypt.png UBH-Vernal WiFi.png
Uintah Basin Healthcare 164.312(e)(1)-(2)(ii), SC-8(3) SC-11-13 SC-40 SI-4(14) SI-8 AC-18 (1) Transmission Security	**Section:** technical **Specification:** Encryption - Wireless Networks **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) for wireless networks and wireless encryption (Must be: AES, 3DES or EES)? **Included Comments:** Wireless LAN uses 802.1X (RADIUS and AD Integration) or WPA2-PSK. HIPAA One Analysis:11.3.2021 **Attachments:** Network Management Policy 2.2.pdf UBH WiFi 1.png UBH WiFi 2 encrypt.png
Organization 164.314(a)(2)(i)(A)-(C), 164.314(a)(2)(ii)-(iii), AC-20-21 CA-3 PM-24 PS-6-8 SA-9 Business Associate Contracts	**Section:** organizational **Specification:** Business Associate Contracts **HIPAA One® Question:** Does the organization's Business Associate Agreement (BAA) contain the required components for your vendors to take responsibility for protecting your ePHI, including the obligation to likewise obligate their sub-contractors to notify you immediately if they have a breach and to take responsibility (legal and practical) by terminating agreement where warranted and/or reporting the problem to the HHS Secretary? This includes the vendor maintaining their own HIPAA/HITECH Act security measures. **Included Comments:** Reviewed/Updated policies 10/21 PM HIPAA One Analysis: 11.3.2021 PM PM 2022 **Attachments:** Business Associates Agreement.doc HIPAA Business Associate Agreement 8 7 13.doc
Organization 164.316(a),(b)(1), PL-1-2 PL-9 Policies and Procedures	**Section:** organizational **Specification:** Documentation **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place that have all the Security and HIPAA-related actions and activities, Policies and Procedures documented, updated and stored in a single location? **Included Comments:** Reviewed/Updated policies 10/21 PM HIPAA One Analysis: 11.3.2021 PM PM 2022 **Attachments:** ITS Security Policy 1.3.pdf

Organization 164.316(b)(2)(i), AU-11 PL-1 Policies and Procedures	**Section:** organizational **Specification:** Time Limit **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place to retain its risk assessment or compliance audit related documentation for at least 6 years from creation? **Included Comments:** Reviewed/Updated policies 10/21 PM HIPAA One Analysis: 11.3.2021 PM PM 2022 **Attachments:** ITS Security Policy 1.3.pdf
Organization 164.316(b)(2)(ii), PL-1 PL-4 PL-9 PS-1 Policies and Procedures	**Section:** organizational **Specification:** Availability **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place that includes that all HIPAA related Policies and Procedures are available to those persons responsible for implementing these procedures? **Included Comments:** Reviewed/Updated policies 10/21 PM HIPAA One Analysis: 11.3.2021 PM PM 2022 **Attachments:** ITS Security Policy 1.3.pdf
Organization 164.316(b)(2)(iii), PL-2(d) PM-1(c) PS-1 Policies and Procedures	**Section:** organizational **Specification:** Updates **HIPAA One® Question:** Does the organization have a Policy and Procedure (PnP) in place to ensure the Policy and Procedures and documentation are periodically reviewed and updated as needed in response to changes in the security of ePHI? **Included Comments:** Reviewed/Updated policies 10/21 PM HIPAA One Analysis: 11.3.2021 PM PM 2022 **Attachments:** ITS Employee Account Policy 4.2.pdf ITS Security Policy 1.3.pdf
Uintah Basin Healthcare Cerner 170.314(d)(4), IP-3 Amendments	**Section:** organizational **Specification:** Corresponding Certification and Standards Criteria **HIPAA One® Question:** Does this certified Electronic Health Record Technology (CEHRT), or EMR software, allow its users to edit or change any part of a patient's chart as requested by the patient (this is called a "patient amendment")? **Included Comments:** KV 10/05/21 HIPAA One Analysis:11.3.2021 PM PM 2022 **Attachments:** patient request 2.PNG patient request.PNG